Supremasi Hukum: Jurnal Kajian Ilmu Hukum, ISSN: 2548-4729 (e) | 2302-1128 (p)
https://ejournal.uin-suka.ac.id/syariah/Supremasi/
Vol. 11, No. 2, 2022, pp. 203-234

Optimizing Personal Data Protection Legal Framework in Indonesia (a Comparative Law Study)

Yuliannova Lestari
Political and International Studies
Central China Normal University
E-mail: yuliannova@mails.ccnu.edu.cn

M. Misbahul Mujib
Fakultas Syariah dan Hukum, UIN Sunan Kalijaga Yogyakarta
E-mail: misbahul.mujib@uin-suka.ac.id

Abstract:
This study explores the protection of personal data-appealing discourse these days. Globally, 132 countries already have special arrangements to protect personal data. The Bill on the Protection of Personal Data in Indonesia is already in the National Legislation Program. Indonesia does not yet have special regulations regarding protecting personal data. Furthermore, it also discussed personal data protection regulations in several countries, both Europe and Asia. This study uses a comparative study that compares personal data protection among countries for further studies on what matters should be included in the Data Protection Bill for Indonesia. The study showed that personal data protection arrangements certainly differ. Most Data Privacy Protection regulates the same stuff, such as principles, protection mechanisms, rights of data subjects, transfers to third countries, and sanctions. It also showed that the regulation of Personal Data Protection in Indonesia is still not adequately controlled compared to the regulations in other countries

Keywords: *Cyber Law, Data Protection, Indonesia, Privacy, Regulations*

Introduction

The development of information and communication technologies has increased rapidly. Enhancing the quality of life in Indonesian society through information technology and research is a national and global concern. The rapid growth of ICT is triggering changes in behavior and attitudes that the Indonesians and the global community are unaware of.[1] These developments created a borderless world where anybody may access anything through the internet. The evolution of information and

[1] Asian Development Bank Ministry of Finance of Republic of Indonesia, *Innovate Indonesia: Unlocking Growth Trough Technological Transformation* (1st edn, Asian Development Bank 2020) 4-6

communication technology opens up new opportunities and poses new challenges.

It is a mode of information and electronic communication that facilitates the delivery of services and goods such as e-commerce. It includes trade and business conducted either through electronic instruments, education, health, e-government, e-payment, transportation, and tourism, and the development of cloud computing, which is essentially apps that provide customer support. Personal information such as a name, e-mail account, and phone contact is becoming more significant in business. A digital dossier is one of the most common types of personal data collected by private companies utilizing internet technology.[2]

As the need for ICT increases, so do the risks of criminal activity. Given the ease with which personal data may dispatch through technology, the danger of personal data leaking has become a significant issue as internet usage has grown.[3] Computing and the internet have made information more accessible. The essential concept of personal data protection was first stated in about 1960s. Frequently, data protection is equated with privacy protection.[4]

The principle of protection in a legal system is stated in the Declaration of Independence, among other places. The statement asserts that God created humanity free and endowed them with certain inalienable rights protected by law. The judiciary defends the community, ensuring the country's high targets are accomplished and maintained. Alan Westin defined privacy as the right of people, organizations, or companies to identify whether or not information about them is shared with other parties.[5] The right to protect personal data and to be justified in data breaches is a civil-liberties.

The right to privacy includes the choice to refuse to provide private information. Hence collecting and distributing personal information is illegal. Personally, identifiable data is a significant economic asset. As the number of mobile phone and internet users expanded, the problem of data protection and privacy became more critical. Many cases have emerged that showcase

---

[2] Sugeng and Annisa Fitria, "Legal Protection of E-Commerce Consumers Through Privacy Data Security" (2021) Proceedings of the 1st International Conference on Law and Human Rights 2020 (ICLHR 2020) 2-4.

[3] Lori N. K. Leonard and Timothy Paul Cronan, "Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences" (2001) 1 Journal of Association for Information Systems 3

[4] Martin Campbell-Kelly and Daniel D Garcia-Swartz, "The History of the Internet: The Missing Narratives." (2013) 28 Journal of Information Technology 20-21

[5] Ali ALibeigi and others, "Right to Privacy, a Complicated Concept to Review"" [2019] Library Philosophy and Practice (e-journal) 3

the importance of developing legal standards to protect personal data. In September 2019, tens of millions of passenger data records from *Lion Air* and *Batik Air* were leaked. In May 2019, customer data from *Malindo Air* and *Thai Lion Air* was exposed, including ID cards and passport numbers stored in *Amazon Web Services* cloud storage.[6] In May 2021, the public was shocked by a data breach affecting over 200 million Indonesians. Acme hackers have stolen and sold Indonesian individuals' data from the National Health Insurance Agency (BPJS). The offers emerged from an internet hacker forum where a guy named Kotz claimed to have 279 million people's data, including extensive personal information. Kotz proposed to provide access to such data in consideration for two bitcoins (roughly 1 billion rupiahs).[7]

Another example of contempt for privacy is displaying a message expressing a commercial, also known as Location-Based Messaging. Occasionally, the message is automatically conveyed to the intended recipient. It is unlikely that they genuinely agreed to let the company monitor their entire activity. The publics have a right to determine whether or not to share private data, and if they do, what requirements must be accomplished by society. Most application servers request personal information such as full names, email addresses, social media accounts, and even account numbers, one of which is to ensure that user data is valid. There is no guarantee that personal information will be kept safe. Account information, home address, bank account hacking, and robbery may be used to commit fraud.

In Indonesia, there are no specific guidelines ruling data privacy protection. Hence it is governed by several laws and regulations that do not follow data protection principles. Indonesia currently lacks explicit rules and regulations on protecting data privacy. To address the issues listed above, the Indonesian government must secure the public, manage personal data protection, and provide legal protection. Criminal activities motivated by the publication of personal data emerge both within the network, through social media, computing cloud, and outside the network, through digital dossier, direct marketing, and others. Additionally, Law No. 17 of 2007, relating to 2005-2025 Indonesia's Long-Term Development Plan stipulates that increasing the utilization of science and technology is essential to strengthening the country.

---

[6] Rizki Fachriansyah, 'Lion Air Leak Puts Data Protection In Spotlight' (*thejakartapost.com*, 2019) <https://www.thejakartapost.com/news/2019/09/19/lion-air-leak-puts-data-protection-in-spotlight.html> accessed 18 April 2022.

[7] A. Muh. Ibnu Aqil, 'Alleged Breach Of BPJS Data Points To Indonesia's Weak Data Protection: Experts' (*thejakartapost.com*, 2021) <https://www.thejakartapost.com/news/2021/05/23/alleged-breach-of-bpjs-data-points-to-indonesias-weak-data-protection-experts.html> accessed 16 April 2022.

It is essential to analyze the current situation of the difficulties and challenges related to data privacy protection and the government oversight of data privacy in Indonesia, including how to control personal data privacy protection in different countries. This research aims to compare the concept of personal data privacy protection and its policy across countries.

Research Methods

Normative legal research identifies lawful norms, judicial principles, and lawful philosophy to resolve legal issues. The argument, hypothesis, or novel notion that emerges from the study of law serves as a prescription for resolving problems. This research is affected by the existing condition of personal data protection legal frameworks, which creates uncertainty.[8] The approach comprises a legal framework, evaluating legal requirements relating to personal data protection, and conceptual.

Examining legal science perspectives and understandings that may assist authors in generating ideas to develop an understanding of legal concepts and principles relating to the issues researched. Specifically, the notion of personal data protection and a comparative approach, comparing personal data protection arrangements in a comparable legal environment. The method of compiling core legal resources, secondary legal materials, and tertiary legal elements in legal books and monthly publications in compliance with the legislative hierarchy.

Privacy and Personal Data Protection

The concept of privacy is universal and regulated by legal and cultural values in many countries. According to Samuel and Brandeis, the legal term for the right to privacy is the right to be left alone, with the definition following: personal dignity, concepts such as human rights, individuality, and independence. Numerous later cases highlighted the importance of preserving the right to privacy, particularly for moral reasons.[9] According to Carolyn Doyle and Mirko Bagaric, the right to privacy concerning personal data is also a legal concept to integrate an individual's right to liberty with their freedoms.[10] Meanwhile, Eliza Watt claims that persistent privacy

[8] Peter Mahmud Mazurni, *Penelitian Hukum* (1st edn, Prenada Media 2015).

[9] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 195-197

[10] Carolyn Doyle and Mirko Bagaric, "The right to privacy: appealing, but flawed" (2006) 9 The International Journal of Human Rights 10-12

violations include interfering with the right to privacy, the right to privacy, and the right to privacy.[11]

According to Moore, the term 'privacy' is complex to describe. It is a condition or a moral demand on others to abstain from particular actions, showing an explicit knowledge of the concept of privacy, which emphasizes its necessity and severity. A privacy state is a phenomenon of being unreachable to a person. In other words, privacy enables people to minimize the ability of others to access their identity and personal data. In a civil society, privacy is highly valued, and individual preferences are socially determined.[12]

Additionally, Arthur Miller highlights privacy as the capacity of people to assert power over the disclosure of personal details. Meanwhile, Ruth Gavison defines privacy as a multifaceted term comprised of three distinct and related components: secrecy and stillness. Because each of these aspects is distinct, each might cause disruption or damage.[13] This is in keeping with Daniel J. Solove's subsequent argument that privacy covers families, physique, sexuality, residence, communication, and personal details.[14]

In addition, Julie Inness represents the private as the context in which a person has authority over the domain of their personal choice, which encompasses rulings on restricted access, private data, and private activities. However, private is defined as the result of affection, like, and regard for everybody else.[15] The ASEAN Human Rights Declaration regards personal data protection as a fundamental right to privacy.[16] Currently, 75 countries have implemented laws concerning data protection.

As for different meanings of privacy offered, a few polarizations have arisen, defining privacy as people's concerns, abilities, or rights to decide what details about themselves may be transferred to everyone else. Additionally, privacy is a measure of a person's control over several aspects

[11] Eliza Watt, "'The right to privacy and the future of mass surveillance'" (2017) 21 The International Journal of Human Rights 775-776

[12] Mark Tunick, "Privacy Rights: Moral and Legal Foundations by Adam D. Moore" (2011) 37 Social Theory and Practice 511-512

[13] Ruth Gavison, "Privacy and the Limits of Law" (1980) 89 The Yale Law Journal 421

[14] Daniel J. Solove, "Conceptualizing Privacy" (2002) 90 California Law Review 1087

[15] Sionaidh Douglas-Scott, "Privacy, Intimacy and Isolation. by Julie Inness" (1993) 102 Oxford University Press 655–658

[16] Nicholas Doyle, "The ASEAN Human Rights Declaration and the Implications of Recent Southeast Asian Initiatives in Human Rights Institution-Building and Standard-Setting" (2014) 63 International and Comparative Law Quarterly 69-70

of his or her personal life, including personal information; the secrecy of self-identity; and parties who have perceptual access to the user or person.

The protection of personal data answers one of the problems of individual privacy rights. As previously explained, personal data is one part of the right to privacy. In this circumstance, personal data protection has gained significant attention from the international community. Human rights are fundamental because they involve human autonomy or authority, are protected by international, regional, and national laws, and have been categorized under human rights arrangements. Personal data is essential to be protected because personal data contains a person's identity and is owned by that person.

With that data, that person can carry out legal actions, make online purchases, a teleconference to chat, and examine witnesses in some instances. Following the theory of legal protection, the law aims to integrate and coordinate various interests in society because, in the traffic of interests, protection of particular interests can be done by limiting various interests on the other hand. Therefore, legal protection is needed to protect personal data from a crime or misuse of personal data itself. The personal data that we/users collect into electronic systems is confidential and must be protected. The operator of the electronic transaction system is obliged to maintain the integrity and confidentiality of the data, which aims to protect the data from hackers and ensure that it is not misused.

The applicator should double-check personal data, for example, by contacting the personal data owner, because nowadays, there are many online fraud modes. Individuals can quickly get their data on the internet and use it as if it were theirs. The purpose of personal data protection law was formed because of the need to protect individual rights in the community in connection with the processing of personal data, whether done electronically or manually, using data processing devices. Adequate personal data protection will give the public confidence to provide personal data for the broader public interest without being misused or violating their rights.

Thus arrangement will balance the rights of individuals and communities whose interests are represented by the state. This regulation regarding personal data protection will significantly contribute and progress in the information society. As well as protecting and guaranteeing the fundamental rights of citizens related to personal protection, corporations, business actors, and organizations. encourage the growth of the digital economy and the information and communication technology industry, and support the improvement of the competitiveness of the domestic industry.

General Data Protection Regulation (GDPR) – European Union

Privacy regulations are legal frameworks that regulate collecting, storing, processing, releasing, and distributing persons' personal information, either online or offline. This legal framework in Europe attempts to defend consumers' fundamental right to life generally and the human right to data privacy in specific. These rights are protected in Europe by two agreements following the European Convention on Human Rights and the European Union Human Rights Council.

The GDPR is a system of legislation intended to enhance personal data protection and establish uniformity in the implementation of protections throughout the European Union. In 1995, the European Union's Council of Ministers adopted a draft regulation known as Directive 95/46/EC of the European Parliament and the Council on the Free Movement of such Data. This regulation was a breeze before the existence of smartphones and social media offered by the government for free internet users. EU regulations extend the privacy protections of the previous directive and implement protective measures in response to emerging technological developments.

In 1970, Germany became the first government to implement a data privacy act. The German Constitutional Court declared in 1983 that every citizen has the right to restrict the use of data privacy and classified data privacy protection as a kind of citizen's right. Thus, the German government brought awareness and established a significant provision in the constitution regarding the universal data protection rules as a fundamental right to privacy controlled by an individual.

This regulation applies to all parties overseas who obtain, manage, and utilize the personal data of EU residents or citizens. The GDPR emphasizes that everybody has authority over the privacy of their data in the presence of external parties through stringent regulation and the imposition of substantial penalties. Everyone includes everybody living in the EU, citizen or not. The GDPR regulates European citizens, businesses, organizations, and government entities abroad that handle and utilize the personal data of all European Union residents. The GDPR was affected on May 25, 2018, replacing the European Union Data Protection Act of 1995.

GDPR is more comprehensive than earlier personal rights or data protection legislation, such as the European Union Data Protection Act of 1995. GDPR applies to organizations or businesses that protect private data and are founded in the European Union, as stated in paragraphs 3 and 4. The GDPR may also apply to firms that handle personal data and are based entirely outside the European Union in certain instances.

The DPA 1998 requires data privacy protection to acquire consent to avoid data usage violations that may affect the data owner. Additionally, the

rule prohibits the transfer of data information even out of Europe unless the receiving country certifies that the data is protected and is not an enterprise. An essential concept in the DPA 1998 is that personal information must be aligned with its legal purpose. Private data must not be retained beyond its registration.

The strategy for managing personal data must comply with its rights. The GDPR aims to harmonize and modernize the architecture for the single online market, empower people in charge of their privacy, and construct contemporary data protection management. Specified categories of personal data, such as information about an individual's ethnic, political preferences, beliefs, trade union membership, medical record, sexual orientation, and biological or biometric data, are processed solely to identify that individual.

Personal Data Protection in Indonesia

Nowadays, data privacy protection in Indonesia is inadequate, considering the lack of a specific regulation. Protecting human rights is expressly regulated in Indonesia's constitution. Nonetheless, the Republic of Indonesia's 1945 Constitution specifies a variety of personal information freedoms. The right to privacy is incorporated in the right to habeas corpus, freedom of belief, freedom of speech, and other comparable rights guaranteeing personal protection. Existing laws and regulations that protect individual privacy are based on these rights. Aside from constitutional rights, Indonesia's Law No. 12/2005 demonstrates the government's commitment to protecting citizens' privacy was the ratification of the International Covenant on Civil and Political Rights.

It is also persistent with Human Rights Law No. 39 of 1999, which contains multiple provisions guaranteeing people's right to privacy. Article 29, paragraph (1), generally stipulates that all citizens have the right to personal, family, honor, dignity, and property protection. [17] Protecting personal information or data is not just a crucial indirect relationship. According to Article 14 (2), one of the rights to self-development is the right to seek, receive, store, process, and transmit information using all available facilities.[18] Article 31 of the Human Rights Law also guarantees secrecy in electronic communications unless a court or other legal authority orders otherwise.[19]

According to the gross domestic product (GDP) rank, Indonesia is the biggest economy in Southeast Asia and the 16th largest economy globally. Being the country's fourth most populous nation, Indonesia has vast potential in the economic sector and the digital environment. According to

[17] Indonesia's Human Rights Law No. 39 of 1999, Article 29
[18] Indonesia's Human Rights Law No. 39 of 1999, Article 14
[19] Indonesia's Human Rights Law No. 39 of 1999, Article 31

Datareportal, in January 2020, Indonesia had 338.2 million mobile connections, 175.4 million internet users, and 160.0 million social media users.[20] However, these possibilities heighten the difficulty of personal data protection (PDP). Some cases, particularly those involving the leakage of personal data related to fraud, emphasized the significance of establishing legal measures to protect data privacy.

Personal data protection in Indonesia is linked to privacy, precisely protecting personal integrity and dignity. Individuals have the right to know who has their information and its utilization. Personal data is an asset or commodity of significant economic value, and its acquisition and distribution violate the right to privacy. Hence, there is a correlation between trust and data privacy protection. Unfortunately, privacy and PDP is not yet regulated in a separate law but are still scattered in various legislations.

Indonesia currently lacks adequate personal data protection legislation. Several regulations rule the protection of personal data in various areas. Personal data protection is governed by Law No. 11 of 2008 on Information and Electronic Transactions, as modified by Law No. 19 of 2016; Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions; and Ministerial Regulation No. 71 of 2019. The previous rules and regulations contain general requirements for processing personal data through electronic systems.

Many sectoral regulations deal with data information and privacy. It includes the Criminal Code, which provides for clauses that persecute breaches of privacy and state secrets that contain personal data exploitation or disclosure, and the Telecommunications Law No. 36 of 1999, which mandates telecommunications service providers to keep confidential any documents or information given by their clients.

Starting in 2016, the Indonesian government initiated a bill on the PDP prepared by the Ministry of Communication and Information as a National Legislative Priority Program. Finally, in January 2020, President Joko Widodo presented the long-awaited final draft of the Indonesian draft law to the Indonesian House of Representatives. If enacted, the PDP Bill will be Indonesia's first personal data protection legal framework established by the DPR this year. Indonesia will therefore become the sixth ASEAN nation to adopt Personal Data Protection Regulations.[21] probably to have affected the scope of this personal data protection bill.

[20] DataReportal Global Digital Insights, 'Digital 2020: Indonesia' (*datareportal.com*, 2020) accessed 18 April 2022.

[21] Indra Arief P and Mecca Yumna, 'President Jokowi Highlights Grave Concern For Personal Data Protection' (*antaranews.com*, 2021)

In the final draft PDP Bill, the terms' control' and 'process' are defined similarly to how they are described in the GDPR. Indeed, the Ministry regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems does not refer to it. Personal Data Subjects must be physical individuals, according to the Final Bill. This final draft bill consists of the definition and classification of personal data, the processing of personal data, the requirements of data controllers and processors when processing personal data, the transfer of personal data, administrative penalties, the prohibition of certain kinds of personal data, the establishment of a code of ethics for regulating personal data, the resolution of disputes about the use of personal data, international cooperation, the role of government and society.[22]

There are many more pieces of personal data protection law in Indonesia. Indonesia has various privacy laws, although they are inconsistent and closed. As Indonesia's first piece of law addressing the protection of personal data in electronic and non-electronic systems, this PDP bill supports the rights and responsibilities of all parties involved. Personal data protection laws and regulations include collecting, storing, exploiting, and disclosing personal information. These laws and regulations may be grouped as follows: telecommunications and information technology; population and archives; finance, banking, and taxation; commerce and industry; health services; and security and law enforcement.

The most significant feature of the final PDP bill was the missing of something often recognized as a crucial component of data privacy law: a distinct, specialized (typically independent) data protection authority, or DPA. Greenleaf claims that just ten of the 143 countries with data privacy laws abolish distinct DPA. The primary advantages of adopting DPA have concentrated knowledge, attention, and specific enforcement responsibilities.[23] The ministerial law enforcement authority is a defining feature of Indonesia's existing data privacy regulations and has been an egregious failure. The Minister has not enforced in seven years, except to issue cautions. This law may also be disregarded unless a DPA is assigned to enforce it.

The Indonesian government has accomplished several versions of the data privacy law, including a specific DPA. The Public Information

<https://en.antaranews.com/news/203849/president-jokowi-highlights-grave-concern-for-personal-data-protection> accessed 18 April 2022.

[22] Article 1, Paragraph 29 of GR 71/2019

[23] Graham Greenleaf, "2014-2017 Update to Graham Greenleaf's Asia Data Privacy Laws – Trade and Human Rights Perspectives" [2017] University of New South Wales Law Research Series 5

Commission will represent DPA in the most recent proposal, combining data privacy obligations with broad Freedom of Information responsibilities. However, few central Ministries opposed it, claiming that Indonesia had too many different institutions that did not work correctly but was too costly to run.

There are some differences and similarities between Indonesia and GDPR, such as: first, the Personal Data Protection Bill does not yet contain regulations regarding the existence of an independent supervisory agency to control data protection. To avoid conflicts of interest, supervisory agencies must ensure that data controllers are not only private institutions. Indonesia does not fulfill the standards for adequate protection due to the lack of an independent institution. Meanwhile, the European Union must create at least one public body in each nation to supervise this legislation's implementation and serve customer data. The government may develop the authority transparently through the legislative and the executive. As stated in article 53 of the GDPR, a person designated as a member of the data protection oversight must have the necessary credentials, experience, and skills in data protection. Therefore posts cannot be given to people who do not have a decent understanding of the digital field.

Second, in the European Union, personal data and privacy protection have been recognized as fundamental rights in the European Union Charter of Fundamental Rights. As a result of the Charter, the European Union enacted new personal data protection laws in 2016 to guarantee personal data in the digital era. The GDPR is an EU law based on Regulation 2016/679. The legislation is fundamentally a step toward strengthening the fulfillment of the European Union's fundamental rights in the digital age. It will directly influence the incentive for economic growth in the digital era. In this instance, Indonesia may include parts of the GDPR's requirements in the Personal Data Protection Bill. Third, the Personal Data Protection Bill regulates the responsibilities of personal data controllers, although GDPR regulates it by using the term Data Protection Impact Assessment (DPIA). Controlling capability, or data processing as specified in the Personal Data Protection Bill and GDPR. The use of personal data is prohibited under the GDPR Personal Data Protection Bill.

The Personal Data Protection Bill will be Indonesia's first comprehensive data protection policy. By acknowledging the rights and responsibilities of the parties involved, not just by electronic but also non-electronic methods, The GDPR-affected data owner rights and the duties of data controllers and processors will make it one of the essential stringent data privacy regulations. However, in the absence of a specific Data Protection

Authority, such regulations are unlikely to be successfully enforced, increasing the possibility that data controllers and users would violate them.

Indonesia currently lacks adequate personal data protection legislation. Personal data protection measures are dispersed beyond various industrial laws and procedures. Due to overlapping norms and regulations, there is no comprehensive and integrated personal data protection framework. Indonesian legislators are now considering a personal data protection policy.

Personal Data Privacy Regulation in Malaysia

One of the principles of regulating personal data in European countries is regulating the flow of personal data in and out and prohibiting personal data from leaving European countries. If the third country does not yet have adequate laws with European countries, it is feared that it will hinder international trade and business which has gone global.[24] To avoid this, the OECD "The Organization for Economic and Cooperation Development" issued a guideline known as "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data".[25]

The Organization for Economic and Cooperation Development (OECD) is an international organization engaged in economic cooperation and development. In Indonesian, the OECD international organization is also called the organization for economic cooperation and development. The purpose of establishing the OECD or organization for economic cooperation and development is to strengthen cooperation and economic development between countries in order to realize sustainable economic stability.[26] The OECD, or the economic cooperation and development organization, now has 38 member countries. Most of the OECD member countries are developed countries, but several developing countries are also members of it.[27] Protection of personal data The Organization for Economic and Cooperation Development (OECD) took part by issuing a guideline for

[24] Sinta Dewi, 'Model Regulation for Data Privacy in the Application of Biometric Smart Card' (2017) 4 Brawijaya Law Journal

[25] Ian J Lloyd, *Information Technology Law* (1st edn, Oxford University Pers 2014).

[26] Organisation for Economic Co-operation and Development OECD, 'OECD Guidelines On The Protection Of Privacy And Transborder Flows Of Personal Data - OECD' (*Oecd.org*, 2018) <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 27 May 2022.

[27] Edison Tabra, 'Corporate Governance In The Organization For Economic Cooperation And Development (OECD) And Its Influence On The Code Of Good Corporate Governance For Peruvian Corporations' (2020) 22 Journal of Applied Business and Economics.

basic principles in protecting personal data that can be used as a reference in making a rule.

Malaysia's Personal Data Protection Act or the Personal Data Protection Act 2010, has several principles in it. the principles of personal data protection that must be complied with are contained in Section 5 (1) of the Personal Data Protection Act 2010 The 709-by the integrity of personal data.[28] A data user's processing of personal data shall comply with the following personal data protection principles: general principle; notice and choice principle; disclosure principle; security principle; retention principle; data integrity principle; and access principle.

In current developments, the need for Personal data protection laws are increasingly pressing. This law must complete the protection of personal data whose settings have been alluded to in several articles in other laws and regulations. In addition, this protection is needed to protect individual rights in the community with the rise of unlawful acts related to personal data such as collection, management, processing, and dissemination of personal data. This is also needed to give public trust in providing personal data and information for the greater public interest without worrying about abuse actions that violate their personal rights.[29] Until now, Indonesia's personal data protection law is still at the drafting stage in the form of a draft law (RUU).

The advantages can be applied in Indonesia by using the comparisons described in the previous chapter. The organization for Economic Cooperation and Development (OECD), which became one of the references in creating the Personal Data Protection Act 2010 (PDPA Malaysia), provides eight principles that must be matched to protect personal data comprehensively.[30] This principle is a basic principle, so it can be applied in Indonesia in several ways, modifications, and changes that can be adapted to the needs and circumstances of the people in Indonesia. Likewise, Malaysia's Personal Data Protection Act 2010 adopts several principles, one of which is the principle issued by the Organization for Economic Cooperation and Development (OECD).

As a reference basis for the protection of personal data, one more principle is added to adjust to the legal situation in Malaysia. In Malaysia's

[28] Section 5, Article 1, Personal Data Protection Act 2010 (PDPA)

[29] Sinta Rosadi, 'Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia' (2018) 5 Brawijaya Law Journal.

[30] Personal Data Protection Commissioner Malaysia, 'PDP Code Of Practice - For Licensees Under The Communications And Multimedia Act 1998' (*pdp.gov.my*, 2017) <https://www.pdp.gov.my/jpdpv2/assets/2019/09/Communications-Sector-PDPA-COP.pdf> accessed 27 May 2022.

Personal Data Protection Act 2010 there is a rule that the application for registration requires everyone to register before managing personal consumer data. In addition, there are provisions governing the transfer of personal data across borders, namely, personal data that can be managed across countries, requiring that country to have a high level of security or at least equivalent to the protection of personal data in Malaysia. Then the provisions regarding sanctions in the Personal Data Protection Act 2010 Malaysia against anyone who violates personal data protection is stated expressly with civil sanctions and criminal sanctions.

Personal Data Privacy in Singapore

The Law protects Personal Data of Customers Personal Data in Singapore on the Protection of Personal Data No. 26 of 2012 Singapore (PDPA 2012 Singapore). Singapore's 2012 PDPA and the 2018 Public Sector Governance Act include the Consent Principle, the Purpose Principle, and the Fairness principle. The user data collected from the Trace Together application above is protected by the Public Sector Governance Act 2018 (hereinafter referred to as PSGA) where data security provisions are included in the Act.[31] The establishment of the PSGA aims to further strengthen public sector data governance while facilitating data sharing between institutions to improve policy-making and service delivery. For privacy data protection practices in Singapore itself, in carrying out the enforcement and effectiveness of applying this rule, presents the Personal Data Protection Commission (PDPC).[32]

The user data collected from the Trace Together application above is protected by the Public Sector Governance Act 2018 (hereinafter referred to as PSGA), where data security provisions are included in the Act. The emergence of the PSGA is aimed at further strengthening public sector data governance while facilitating inter-agency data sharing to improve policy-making and service delivery. The PSGA stipulates the criteria for data that can be shared with all public bodies.[33] The PSGA also imposes criminal penalties on public officials who recklessly or intentionally disclose data without permission, misuse data for profit, or re-identify data.

Anonymized as in Section 7 of the PSGA. In the explanation of section 7 of the PSGA, it is stated that an individual who causes disclosure of

[31] Benjamin Wong Yong Quan, 'Data Privacy Law In Singapore: The Personal Data Protection Act 2012' (2017) 7 International Data Privacy Law.

[32] Vili Lehdonvirta, 'European Union Data Protection Directive: Adequacy Of Data Protection In Singapore' (2004) Singapore Journal of Legal Studies.

[33] Terence Lee and Howard Lee, 'Tracing Surveillance And Auto-Regulation In Singapore: 'Smart' Responses To COVID-19' (2020) 177 Media International Australia.

data (data leakage), intentionally or unintentionally, under the control of the Singapore public sector, can be sentenced to imprisonment of up to 2 years or a fine of $5000 (Singapore dollars).[34] The application of criminal penalties in Singapore in case of data leakage, especially in the public sector (government), can be said to be more effective, at least when compared to the rules in Indonesia which only apply administrative sanctions and are still limited to ministerial regulations. Even though the crime is an *ultimum remedium*, it can be seen as quite effective in providing a deterrent effect against perpetrators of misuse of privacy data. For privacy data protection practices in Singapore itself, the Personal Data Protection Commission (PDPC) is presented in carrying out the enforcement and effectiveness of this rule.

The main task of this commission is at least as a compliance monitor in the implementation of this rule, in addition to being authorized to receive complaints from the general public and as a facilitator in alternative dispute resolution. Any individual who suffers a loss due to the misuse of privacy data by an organization that has an obligation to protect privacy data, such as in the case of implementing digital contact tracing, can file a lawsuit against the responsible organization. civilly. Furthermore, anyone who suffers a loss can file a complaint with PDPC Singapore on suspicion of misuse of their privacy data by the organization. PDPC Singapore can also conduct an investigation after receiving a complaint and it is possible to impose sanctions in the form of a fine of up to S$1 million if there is sufficient evidence that the organization has violated the rules of the PDPA. Sanctions that can be imposed in addition to fines, namely sanctions in the form of imprisonment for a maximum of three years as stipulated in Section 56 of the PDPA.[35]

Compared to Indonesia and Singapore, this neighboring country already has a form of protection contained in the Personal Data Protection Act and the Public Sector Governance Act. The Singapore government applies criminal sanctions and fines for personal data violations, such as in the event of unauthorized disclosure of data. Meanwhile, in Indonesia, sanctions for This is still limited to administrative sanctions that do not have a deterrent effect for data abusers, this itself is related to data collection responsibility for personal data. For regulations specifically regarding the protection of personal data, in Indonesia it is still limited to Ministerial regulations and scattered in other regulations that are not sufficiently accommodating.

[34] Public Sector Governance Act 2018, Section 7
[35] Personal Data Protection Act 2012, Section 56

Regarding privacy data protection practices in Singapore, it is also good enough to be used as a benchmark for Indonesia, especially with the existence of the Personal Data Protection Commission (PDPC). It is urgent for Indonesia to immediately have a special regulation regulating the protection of its citizens' personal data. Especially in the case of the use of personal data for COVID-19 prevention efforts. Indonesia is expected to follow Singapore's example, which has guaranteed the protection of personal data stated in the Lion Country law, namely PDPA and PSGA.

Personal Data Privacy Ordinance of 1995 – Hong Kong

Hong Kong is the first country to be comprehensively regulated on privacy issues for personal data in Asia. The regulation is known as the Personal Data Privacy Ordinance of 1995 (PDPO). The data privacy protection principle contained in the PDPO cannot be fully implemented. Therefore, in 2012 the Hong Kong government made changes to the PDPO. A particular agency implements these laws and regulations for handling personal data privacy issues, namely the Privacy Commissioner for Personal Data (PCPD). Hong Kong applies six principles of Personal Data Protection for its country: Limitations on collecting personal data; use of personal data; data quality and providing advice to third parties; deletion and destruction of personal data; data security obligations; and practices.

The collection of personal data is limited to the lawful collection of personal data for purposes directly related to the function of the collector. The data collected should be sufficient, but the collection of personal data should not exceed the purpose for which the data was collected. The principles also require all steps to ensure the accuracy of personal data, taking into account the purpose of users and any related purposes and removing or not using inaccurate data. Then the personal data manager is obliged to take every step that supports protecting personal data from access that cannot be taken, or deletion, deletion, deletion, and unauthorized use. These data security measures consider various factors, such as the type of data, the location where the data is stored, and the potential for physical harm to the data. Unlike European law, the PDPO does not provide special arrangements for sensitive data.

The principle of protecting the privacy rights of personal data in Hong Kong includes limitations on data collection that is carried out based on the purpose for which it was legally collected. The use and disclosure of personal data must be under its objectives. The owner's consent, correct quality of personal data, and storage of personal data by third parties have a time limit. Personal data managers are required to protect against irresponsible access and the disclosure of 'data user' used by Hong Kong,

which requires third parties to manage data (organizations or companies) to publish privacy policies to the public. If violated, the Hong Kong government provides a subpoena to the public. The third party is concerned.

Doxing, disclosing prior personal data information to the society without an agreement, frequently through the network has started a prevalent but risky and unalterable method used by communities housing prejudices counter to each other. Within the 2019 Hong Kong demonstrations, both sides participated in doxing to the disadvantage of the other demonstrators opposed the cops, pro-government partisans facing protesters, and their sympathizers.[36] Both parties filed complaints with the PCPD, Hong Kong's privacy authority. However, as most of the disclosed information is hosted outside Hong Kong, authorities lack extraterritorial power to request removal. As a result, the Hong Kong authority amended the Personal Data Privacy Ordinance (PDPO) on July 21 to address doxing. The law should be approved by October. However, the global IT industry's significant players responded quickly and aggressively.[37]

The Asia Internet Coalition, located in Singapore, represents major American internet companies. Such as *Apple, Amazon, Facebook, Google, LinkedIn, and Twitter*, noted to the Hong Kong authority expressing worry about the law's potential to subject their employees to criminal inquiry or punishment for what they write on the internet. Globally, media headlines said these corporations were planning to depart from Hong Kong if the new legislation was implemented.[38]

The privacy commissioner was immediately greeted by video conference with corporate executives in response to their allegations. Carrie Lam, Hong Kong's Chief Executive, took a more strident stance, stating that the businesses' fears were unjustified and would be shown erroneously once the new laws took effect. Only national security law did not provide the circumstances envisioned among those who opposed it. The PDPO for Hong Kong was initially adopted in 1995 and went into force in December

[36] Matt Bower and Clement Sung, 'Data Privacy & Transfer In Investigations: Hong Kong - Global Investigations Review' (*globalinvestigationsreview.com*, 2021) <https://globalinvestigationsreview.com/insight/know-how/data-privacy-and-transfer-in-investigations/report/hong-kong> accessed 27 May 2022.

[37] The Government of the Hong Kong Special Administrative Region, 'Personal Data (Privacy) (Amendment) Bill 2021' (Constitutional and Mainland Affairs Bureau 2021).

[38] Newley Purnell, 'Facebook, Twitter, Google Threaten To Quit Hong Kong Over Proposed Data Laws' (*wjs.com*, 2021) <https://www.wsj.com/articles/facebook-twitter-google-warn-planned-hong-kong-tech-law-could-drive-them-out-11625483036> accessed 17 April 2022.

1996, prior to the territory's transfer to China.[39] It was claimed to be Asia's first integrated data security regulation. By establishing an independent authority, the government assured that its regulatory decisions would be made independently of the government.

An early assessment of the Xinhua Press Agency, China's genuinely delegate in Hong Kong, revealed this independence. Immediately after the rules' passage, objection lawmaker Emily Lau demanded that Xinhua make public anything documents it had on her. The government failed to react to her after the legally mandated time of forty days. The PCPD inspected and merely then did Xinhua give Lau a one-line response, saying that it had no documents on her. In February 1998, just over a year after the transition, the PCPD sent the evidence to Hong Kong's secretary for justice, who refused to testify. That was twenty-three years ago. At the very least, the regulator seemed to have attempted to intervene.[40]

Personal Information Protection Law (PIPL) - China

China's new privacy legislation requires stricter protections for citizens' personal information and may have extraterritorial implications for firms operating outside the nation. The Personal Information Protection Law (PIPL), which was effected on November 1, 2021, will collaborate with China's Cybersecurity Law (CSL) and Data Security Law (DSL) to reach an important mechanism controlling cyber security and data privacy protection in China. The new privacy regulation affects local and global enterprises that handle or utilize personal data from Chinese residents.[41]

PIPL defines personal information, explains the legal basis for personal processing information, defines processor duties and responsibilities, and mandates data localization to protect China's interests when personal

[39] Hong Kong Government, 'The Personal Data (Privacy) Ordinance' (*Pcpd.org.hk*, 2022) <https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html> accessed 27 May 2022.

[40] Selina Cheng, 'Hong Kong Moves To Ease Fears As Industry Group Says Facebook, Google, Twitter May Pull Out Of City Over New Privacy Law - Hong Kong Free Press HKFP' (*hongkongfp.com*, 2021) <https://hongkongfp.com/2021/07/06/hong-kong-moves-to-ease-fears-as-facebook-google-twitter-threaten-to-pull-out-of-city-over-new-privacy-law/> accessed 13 April 2022.

[41] Rogier Creemers and Graham Webster, 'Translation: Personal Information Protection Law Of The People's Republic Of China-Effective Nov. 1, 2021-Digichina' (*digichina.stanford.edu*, 2021) <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> accessed 17 April 2022.

information is transferred across borders.[42] There are many aspects of China's PIPL similar to those of GDPR.[43] The GDPR is one of the world's most important privacy and security legislation. Article 3 explains that the PILP has similarities, such as the GDPR is extraterritorial; includes all citizens, organizations, and companies within China's borders. In addition, chapter IV explained that PIPL empowers customers to gain access to and duplicate their data, request correction of data errors, and withdraw their authorization.[44]

Additionally, the PIPL incorporates several terms and terminology similar to the GDPR. For instance, the PIPL requires any processor of personal information located outside of China to develop a specialized organization or delegate a representative to be accountable for significant personal information cybersecurity threats inside China.[45] Under the GDPR, this personal information processor is analogous to a data controller. A similarity emerges between PIPL and GDPR data processors, or businesses that handle personal data on behalf of the data controllers.[46]

Meanwhile, the PIPL and the GDPR have many similar characteristics. The PIPL departs from the EU's data privacy legislation in some aspects, making it potentially tighter than the GDPR. For example, the PIPL contains a genuine interest in processing reason, the GDPR's most flexible essential precedent for processing personal data.[47] Companies are permitted to handle personal data under the GDPR as long as the data was gathered lawfully and legitimately.[48] With this legal foundation conspicuously absent from the PIPL, corporations doing business in China must get

[42] Yang Feng, "The future of China's personal data protection law: challenges and prospects" (2019) 27 Asia Pacific Law Review 70

[43] European Parliament, "Regulation (EU) 2016/679 of the European Parliament and of the Council Regulation (EU)" (Official Journal of the European Union 2016)

[44] Anjali C. Das, 'China's New Personal Information Protection Law' (*natlawreview.com*, 2021) <https://www.natlawreview.com/article/china-s-new-personal-information-protection-law> accessed 10 April 2022.

[45] China's Personal Information Protection Law, Article 53

[46] Amigo L. Xie and others, 'What Is Required Under The PIPL: A PRC-Based Representative Or A Personal Information Protection Officer?' (*https://www.klgates.com/*, 2022) <https://www.klgates.com/What-is-Required-Under-The-PIPL-A-PRC-Based-Representative-or-a-Personal-Information-Protection-Officer-1-7-2022> accessed 10 April 2022.

[47] Cooley Alert, 'China's New National Privacy Law: The PIPL' (*cooley.com*, 2022) <https://www.cooley.com/news/insight/2021/2021-11-30-china-new-national-privacy-law> accessed 16 April 2022.

[48] European Union Commission 'GDPR User Friendly Guide To General Data Protection Regulation' (*gdpreu.org*, 2020) <https://www.gdpreu.org/#lawfulness-fairness-transparency> accessed 17 April 2022.

individual permission before accessing their private information, except if the purpose falls under one of the six exclusions in Article 13.[49]

The last exemption provides that parties may treat personal information without the individual agreement in certain conditions specified in applicable legislation and regulatory rules. However, the conditions under which corporations qualify for this exemption remain uncertain. It may allow the Chinese government to expand or contract the PIPL's impact in the future as desired. Furthermore, unlike the GDPR, the PIPL includes a robust data localization provision, demanding that personal information exceeding certain thresholds be preserved within China and that any handover of such data outside the country is subject to a risk evaluation by China's Cyberspace Administration.[50]

The PIPL does not provide a capacity restriction or more information on the security assessment's purpose and evaluation aspects. The PIPL's sanctions are also distinct from the GDPR's. For example, the GDPR establishes a maximum penalty of 20 million Euros, equal to 22.6 million USD or 4 percent of global annual revenue, whichever is more extensive.[51] The PIPL provides a maximum penalty of 50 million Chinese Renminbi, equal to 7.8 million USD or 5 percent of the prior fiscal year's yearly income.[52]

Moreover, PIPL does not indicate whether yearly income in its definition applies to global revenue, as in GDPR, or merely yearly income in China. Compared to GDPR, the PIPL is not significantly different from the GDPR. The vagueness in several clauses gives the PIPL the potential to become a considerably tighter data privacy regulation. Regarding regulation, it is questionable how tightly the PIPL will be implemented and what areas the Chinese government will emphasize. The PIPL's legal status will be determined by the Chinese government's implementation of these rules and the interests that motivate its decisions rather than by their content.

In particular, China's political framework and restrictive internet surveillance policies are distinct from those of major western countries and will almost obviously impact how PIPL is executed. China's PIPL is strongly connected to national protective measures, as illustrated by its enhanced data localization restrictions. In contrast, US and European data privacy laws like

[49] China's Personal Information Protection Law, Article 13

[50] China's Personal Information Protection Law, Article 40

[51] GDPR, 'Art. 83 GDPR – General Conditions For Imposing Administrative Fines' (*gdpr-info.eu*, 2021) <https://gdpr-info.eu/art-83-gdpr/> accessed 16 April 2022.

[52] China Briefing, 'The PRC Personal Information Protection Law (Final): A Full Translation' (*china-brifieng.com*, 2021) <https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/> accessed 15 April 2022.

GDPR focus on individual and consumer rights.[53] However, the PIPL arises during China's massive crackdown on domestic and global private-sector firms.[54] *In recent years, Alibaba, Tencent, and Bilibili have all been penalized for anti-monopoly violation*s.[55] On January 1, 2009, Yahoo discontinued operations in China despite the challenging economic business and legislative, political conditions.[56] LinkedIn also shut down its China section earlier this month, describing a challenging working environment.[57]

The PIPL will undoubtedly cause parties based in China to face significant issues, considering the conditions surrounding its approval. For example, Grindr recently removed its app from the Chinese Apple App Store owing to regulatory issues.[58] In addition, within two weeks of the PIPL taking effect, several local manufacturers in China stopped providing shipping data to international companies. Businesses rely on data to gain insight into shipping quantities and logistics planning.[59] According to PIPL, international businesses should examine regulatory costs and operational breakdowns. Globally, given China's critical role in global supply chain processes and hosting several major container ports, this knowledge gap could affect the global financial system.[60]

---

[53] Condé Nast, 'Ignore China's New Data Privacy Law At Your Peril' (*www.weird.com*, 2021) <https://www.wired.com/story/china-personal-data-law-pipl/> accessed 18 April 2022.

[54] Laura He, 'China's 'Unprecedented' Crackdown Stunned Private Enterprise. One Year On, It May Have To Cut Business Some Slack' (*www.cnn.com*, 2021) <https://edition.cnn.com/2021/11/02/tech/china-economy-crackdown-private-companies-intl-hnk/index.html> accessed 18 April 2022.

[55] Josh Horwitz and Kim Coghill, 'China's Market Regulator Fines Alibaba, Tencent For Failing To Report Deals' (*www.reuters.com*, 2022) <https://www.reuters.com/world/china/chinas-market-regulator-fines-alibaba-tencent-failing-report-deals-2022-01-05/> accessed 18 April 2022.

[56] Deutsche Welle, 'Yahoo Pulls Out Of China Over 'Challenging' Environment' (*dw.com*, 2022) <https://www.dw.com/en/yahoo-pulls-out-of-china-over-challenging-environment/a-59695571> accessed 18 April 2022.

[57] Karen Weise and Paul Mozur, 'Linkedin To Shut Down Service In China, Citing 'Challenging' Environment' (*nytimes.com*, 2021) <https://www.nytimes.com/2021/10/14/technology/linkedin-china-microsoft.html> accessed 18 April 2022.

[58] Paul Mozur, 'Grindr Is Pulled From Apple'S App Store In China.' (*nytimes.com*, 2022) <https://www.nytimes.com/2022/02/02/business/grindr-apple-app-store-china.html> accessed 18 April 2022.

[59] Jonathan Saul and Eduardo Baptista, 'Off The Grid: Chinese Data Law Adds To Global Shipping Disruption' (*www.reuters.com*, 2021) <https://www.reuters.com/world/china/off-grid-chinese-data-law-adds-global-shipping-disruption-2021-11-17/> accessed 18 April 2022.

[60] World Shipping Council, 'Top 50 Ports' (*www.worldshipping.org*, 2019) <https://www.worldshipping.org/top-50-ports> accessed 18 April 2022.

Personal Information Protection Act (PIPA) 2011 – South Korea

In 2020, the regulations were amended to provide data protection rights for South Korean citizens. The Personal Information Protection Act or PIPA, is a South Korean data privacy law Originally passed in 2011.[61] PIPA sets various restrictions on individuals, businesses, and organizations that collect and process the personal information of South Korean citizens. On the other hand, PIPA also stipulates various rights granted to South Korean citizens related to data protection and solutions if data subjects feel as if their rights have been violated.

The PIPA extends to all data controllers located in South Korea, regardless of whether they are individuals, commercial entities, linked third parties, or other organizations that receive, access, process, or disclose personal information about South Korean citizens. [62] Alternatively. In contrast, many other data privacy laws around the world contain specific provisions regarding the territorial scope of those regulations. PIPA does not specify the statutory jurisdiction regarding institutions and individuals processing personal information of South Korean citizens outside South Korean physical boundaries.

However, in practice, the territorial functionality of PIPA has been contended on a case-by-case basis. The South Korean Government evaluates a variety of factors when establishing whether a particular individual or institution must define following the requirements, including whether the company derives revenue from doing business in South Korea or providing services intended explicitly for South Korean citizens. PIPA encompasses the handling of personal data, which is defined as the assemblage, creation, registry, repository, manufacturing, modification, exploration, output, correction, recovery, supply, confession, or damage of data information.[63]

Under the PIPA, many data privacy rights are afforded to South Korean citizens. These various legal rights include:[64]

a. The right to be informed. Although obtaining consent from the data subject, the data handler must provide written notice to the data

[61] Kwang Bae Park and others, "Main Issues in Korea Regarding Consent for the Processing of Personal Information, with Emphasis on Recent Supreme Court Cases" (2017) 17 Journal of Korean Law 61-63

[62] Kang Taeuk and Park Susan, "Transfer of Personal Information in a Corporate Structural Change" (2017) 17 Journal of Korean Law 101-113

[63] Juyoen Lee and Eric Yong Joong Lee, "Personal data protection of academic journals in the age of the European General Data Protection Regulation: guidelines for Korean journals" (2019) 6 Science Editing 73-77

[64] Sangchul Park and others, "Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies" (2020) 323 JAMA 21-24

subject regarding the purposes for which the personal information is collected and used. The specific items of personal information to be collected, the period of retention of such personal information, the right of the data subject to object to their consent to the collection of the data, and any losses that may arise from the refusal.

b. The right to access. According to PIPA, data subjects have the right to request that data handlers provide them with access to personal information held by those data handlers. However, there are circumstances this access may could not be denied, such as when access would cause possible damage to third parties.
c. The right to rectification. In addition to the data subject's right to request access to personal information and has the right to recorrect that information; and The right to erasure. Suppose the data subject is granted access to their personal information, but decides not to remedy it. In that case, They still can request that their data privacy be deleted.

Additionally, suppose data handlers plan to share the personal information of data subjects with third parties. In that situation, they can also notify those data subjects of the identities of external parties who might have access to the data and the individual data to be disclosed. The third parties' purposes for collecting data subjects' personal information are the period the third party will use and retain personal information, the data subjects' right to refuse their consent to data collection, and any disadvantages that may result from refusal. The right to object or opt-out-Data handlers must allow for data subjects to object to our opt-out of the collection and processing of their personal information at any time, as well as respond to a data subject's request to suspend the processing of their personal information after it has been collected.[65]

Furthermore, South Korea joins the recent trend of privacy legislation that continues to grow worldwide as personal information and data are being shared at a rate never seen before. As such, South Korean citizens can rest assured that they have the means to protect the personal information they share with data handlers and receive justice if their personal information is accessed without their consent.

[65] Younsik Kim, "Uncertain future of privacy protection under the Korean public health emergency preparedness governance amid the COVID-19 pandemic" (2022) 8 Cogent Social Sciences 10-11

The Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2015) - Japan

The law on data privacy protection in Japan was first issued in 2003. Indeed, Japan was the first country that implements a personal data protection law in Asia. Rather than replacing the Act, as other legislatures opted to do, Japan overhauled the law in September 2015, following numerous high-profile data breaches.[66]

The new 2015 overhaul introduced the Personal Information Protection Commission (PIPC), an independent agency tasked with protecting the rights and interests of individuals relating to data privacy. It also encourages appropriate and adequate personal data use. Like other data protection legislation, such as the GDPR, the APPI applies to all companies that offer goods and services in Japan, irrespective of their valid location. That is known as an extraterritorial scope. However, recent amendments now mean the Act applies to all organizations marching the data privacy for business purposes, regardless of the number of individuals. Japan amended its data privacy and protection legislation, the Act on the Protection of Personal Information, in June 2021.[67] Affected organizations should examine and modify their security policies and processes to guarantee adherence with the APPI's new regulations and duties by April 2022.

A pioneering omnibus personal and information security legislation, the APPI was first signed into law in 2003. Since 2003, the policy has been revised several times, pushing the issue to step with contemporary privacy concerns and offering customers additional rights while restricting enterprises. Additionally, restricted classifications under the legislation, the most significant APPI ordinance, focuses on further monitoring cross-border data transmission (necessitating opt-in permission), such as personal-related information.

The new updates to the APPI will require companies to take measures to preserve the private data information of the individual concerned, such as introducing a form of pseudonymization. In addition, the APPI will require companies to submit a data breach report to the Personal Information Protection Commission (PPC) and notify individuals concerned about data loss. The latest updates to APPI expand the rights of data subjects, such as cessation of use, deletion, and cessation of third-party provisions of

[66] Flora Y Wang, "Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement" (2020) 33 Harvard Journal of Law & Technology 670

[67] Ministry of Foreign Affairs of Japan, 'Amended Act On The Protection Of Personal Information' (Personal Information Protection Commission 2020).

retained personal data. The updates make it easier for individuals concerned to exercise their privacy rights and broaden the types of retained data. Any data retained for less than six months is included in a data subject right to demand disclosure of data.

As penalties are increased, Japan's privacy law significantly affects both the data subjects (consumers) and data handlers (companies). If a data handler fails to comply with the amended privacy updates, the maximum fine on data handlers can reach upwards of 100 million yen, depending on the violation. An increase in penalties is not the only update to the APPI that holds companies responsible for violating privacy rights; for example, expanding the PPC authority to offshore companies will allow the PPC to report privacy violations.

Conclusion

Based on the previous explanation, it is possible to infer that the regulation of Personal Data Protection in Indonesia is still not adequately controlled compared to the regulations in other countries. Several regulations in Indonesia regulate the protection of personal data, namely the 1945 Constitution of the Republic of Indonesia, Law on Human Right No. 39 of 1999, Law on Electronic Information and Transactions No. 11 of 2008, Government Regulation no. 82 of 2012, and Indonesian Minister of Communication and Informatics (MOCI) Regulation No. 20 of 2016 regarding of personal data as well as several other sectoral regulations. However, some of these regulations appear to be disharmony, so legal unification is needed.

Moreover, the Personal Data Protection Bill has been included in the National Legislation Program of the National Legislation Program since 2019. It needs excellent attention and analysis to design this bill into a solid and fair regulation. The advice that can be identified is the legal harmonization of advanced and in-depth personal data protection. The government needs to create and run like the Data Protection Agency in the European Union, already proclaimed by the existence of a Commission in the Personal Data Protection Bill, firmly and adequately to control the legal relationship between personal data owners and data controllers.

Based on the description above, the authors suggest that the government needs to immediately ratify the implementation of the Personal Data Protection Bill as harmonious and synergistic legislation regarding the Protection of Personal Data and Information. It is the role and responsibility of the State to guarantee human rights, namely the right to privacy and protection, especially in information and communication technology

activities. Of course, it aims to reduce various violations in Data Protection and Personal Information practice.

Daftar Pustaka

A. Muh. Ibnu Aqil, 'Alleged Breach Of BPJS Data Points To Indonesia's Weak Data Protection: Experts' (*thejakartapost.com*, 2021) <https://www.thejakartapost.com/news/2021/05/23/alleged-breach-of-bpjs-data-points-to-indonesias-weak-data-protection-experts.html> accessed 16 April 2022.

Ali ALibeigi and others, "Right to Privacy, a Complicated Concept to Review"" [2019] Library Philosophy and Practice (e-journal) 3

Amigo L. Xie and others, 'What Is Required Under The PIPL: A PRC-Based Representative Or A Personal Information Protection Officer?' (*https://www.klgates.com/*, 2022) <https://www.klgates.com/What-is-Required-Under-The-PIPL-A-PRC-Based-Representative-or-a-Personal-Information-Protection-Officer-1-7-2022> accessed 10 April 2022.

Anjali C. Das, 'China's New Personal Information Protection Law' (*natlawreview.com*, 2021) <https://www.natlawreview.com/article/china-s-new-personal-information-protection-law> accessed 10 April 2022.

Asian Development Bank Ministry of Finance of Republic of Indonesia, *Innovate Indonesia: Unlocking Growth Trough Technological Transformation* (1st edn, Asian Development Bank 2020) 4-6

Benjamin Wong Yong Quan, 'Data Privacy Law In Singapore: The Personal Data Protection Act 2012' (2017) 7 International Data Privacy Law.

Carolyn Doyle and Mirko Bagaric, "The right to privacy: appealing, but flawed" (2006) 9 The International Journal of Human Rights 10-12

China Briefing, 'The PRC Personal Information Protection Law (Final): A Full Translation' (*china-brifieng.com*, 2021) <https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/> accessed 15 April 2022.

Chinese Personal Information Protection Law

Condé Nast, 'Ignore China's New Data Privacy Law At Your Peril' (*www.weird.com*, 2021) <https://www.wired.com/story/china-personal-data-law-pipl/> accessed 18 April 2022.

Cooley Alert, 'China's New National Privacy Law: The PIPL' (*cooley.com*, 2022) <https://www.cooley.com/news/insight/2021/2021-11-30-china-new-national-privacy-law> accessed 16 April 2022.

Daniel J. Solove, "Conceptualizing Privacy" (2002) 90 California Law Review 1087

DataReportal Global Digital Insights, 'Digital 2020: Indonesia' (*datareportal.com*, 2020) accessed 18 April 2022.

Deutsche Welle, 'Yahoo Pulls Out Of China Over 'Challenging' Environment' (*dw.com*, 2022) <https://www.dw.com/en/yahoo-pulls-out-of-china-over-challenging-environment/a-59695571> accessed 18 April 2022.

Edison Tabra, 'Corporate Governance In The Organization For Economic Cooperation And Development (OECD) And Its Influence On The Code Of Good Corporate Governance For Peruvian Corporations' (2020) 22 Journal of Applied Business and Economics.

Eliza Watt, "'The right to privacy and the future of mass surveillance'" (2017) 21 The International Journal of Human Rights 775-776

European Parliament, "Regulation (EU) 2016/679 of the European Parliament and of the Council Regulation (EU)" (Official Journal of the European Union 2016)

European Union Commission 'GDPR User Friendly Guide To General Data Protection Regulation' (*gdpreu.org*, 2020) <https://www.gdpreu.org/#lawfulness-fairness-transparency> accessed 17 April 2022.

Flora Y Wang, "Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement" (2020) 33 Harvard Journal of Law & Technology 670

GDPR, 'Art. 83 GDPR – General Conditions For Imposing Administrative Fines' (*gdpr-info.eu*, 2021) <https://gdpr-info.eu/art-83-gdpr/> accessed 16 April 2022.

Graham Greenleaf, "2014-2017 Update to Graham Greenleaf's Asia Data Privacy Laws – Trade and Human Rights Perspectives" [2017] University of New South Wales Law Research Series 5

GR 71/2019, Paragraph 29, Article 1.

Hong Kong Government, 'The Personal Data (Privacy) Ordinance' (*Pcpd.org.hk*, 2022) <https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html> accessed 27 May 2022.

Ian J Lloyd, *Information Technology Law* (1st edn, Oxford University Pers 2014).

Indonesian Human Rights Law No. 39 of 1999.

Indra Arief P and Mecca Yumna, 'President Jokowi Highlights Grave Concern For Personal Data Protection' (*antaranews.com*, 2021) <https://en.antaranews.com/news/203849/president-jokowi-highlights-grave-concern-for-personal-data-protection> accessed 18 April 2022.

Jonathan Saul and Eduardo Baptista, 'Off The Grid: Chinese Data Law Adds To Global Shipping Disruption' (*www.reuters.com*, 2021) <https://www.reuters.com/world/china/off-grid-chinese-data-law-adds-global-shipping-disruption-2021-11-17/> accessed 18 April 2022.

Josh Horwitz and Kim Coghill, 'China's Market Regulator Fines Alibaba, Tencent For Failing To Report Deals' (*www.reuters.com*, 2022) <https://www.reuters.com/world/china/chinas-market-regulator-fines-alibaba-tencent-failing-report-deals-2022-01-05/> accessed 18 April 2022.

Juyoen Lee and Eric Yong Joong Lee, "Personal data protection of academic journals in the age of the European General Data Protection Regulation: guidelines for Korean journals" (2019) 6 Science Editing 73-77

Kang Taeuk and Park Susan, "'Transfer of Personal Information in a Corporate Structural Change" (2017) 17 Journal of Korean Law 101-113

Karen Weise and Paul Mozur, 'Linkedin To Shut Down Service In China, Citing 'Challenging' Environment' (*nytimes.com*, 2021) <https://www.nytimes.com/2021/10/14/technology/linkedin-china-microsoft.html> accessed 18 April 2022.

Kwang Bae Park and others, "Main Issues in Korea Regarding Consent for the Processing of Personal Information, with Emphasis on Recent Supreme Court Cases" (2017) 17 Journal of Korean Law 61-63

Laura He, 'China's 'Unprecedented' Crackdown Stunned Private Enterprise. One Year On, It May Have To Cut Business Some Slack' (*www.cnn.com*, 2021)

<https://edition.cnn.com/2021/11/02/tech/china-economy-crackdown-private-companies-intl-hnk/index.html> accessed 18 April 2022.

Lori N. K. Leonard and Timothy Paul Cronan, "Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences" (2001) 1 Journal of Association for Information Systems 3

Mark Tunick, "Privacy Rights: Moral and Legal Foundations by Adam D. Moore" (2011) 37 Social Theory and Practice 511-512

Martin Campbell-Kelly and Daniel D Garcia-Swartz, "The History of the Internet: The Missing Narratives." (2013) 28 Journal of Information Technology 20-21

Matt Bower and Clement Sung, 'Data Privacy & Transfer In Investigations: Hong Kong - Global Investigations Review' (*globalinvestigationsreview.com*, 2021) <https://globalinvestigationsreview.com/insight/know-how/data-privacy-and-transfer-in-investigations/report/hong-kong> accessed 27 May 2022.

Ministry of Foreign Affairs of Japan, 'Amended Act On The Protection Of Personal Information' (Personal Information Protection Commission 2020).

Newley Purnell, 'Facebook, Twitter, Google Threaten To Quit Hong Kong Over Proposed Data Laws' (*wjs.com*, 2021) <https://www.wsj.com/articles/facebook-twitter-google-warn-planned-hong-kong-tech-law-could-drive-them-out-11625483036> accessed 17 April 2022.

Nicholas Doyle, "The ASEAN Human Rights Declaration and the Implications of Recent Southeast Asian Initiatives in Human Rights Institution-Building and Standard-Setting" (2014) 63 International and Comparative Law Quarterly 69-70

Organisation for Economic Co-operation and Development OECD, 'OECD Guidelines On The Protection Of Privacy And Transborder Flows Of Personal Data - OECD' (*Oecd.org*, 2018) <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 27 May 2022.

Paul Mozur, 'Grindr Is Pulled From Apple'S App Store In China.' (*nytimes.com*, 2022) <https://www.nytimes.com/2022/02/02/business/grindr-apple-app-store-china.html> accessed 18 April 2022.

Personal Data Protection Act 2012, Section 56

Personal Data Protection Commissioner Malaysia, 'PDP Code Of Practice - For Licensees Under The Communications And Multimedia Act 1998' (*pdp.gov.my*, 2017) <https://www.pdp.gov.my/jpdpv2/assets/2019/09/Communications-Sector-PDPA-COP.pdf> accessed 27 May 2022.

Peter Mahmud Mazurni, *Penelitian Hukum* (1st edn, Prenada Media 2015).

Personal Data Protection Act 2010 (PDPA), Section 5, Article 1.

Public Sector Governance Act 2018, Section 7

Rizki Fachriansyah, 'Lion Air Leak Puts Data Protection In Spotlight' (*thejakartapost.com*, 2019) <https://www.thejakartapost.com/news/2019/09/19/lion-air-leak-puts-data-protection-in-spotlight.html> accessed 18 April 2022.

Rogier Creemers and Graham Webster, 'Translation: Personal Information Protection Law Of The People's Republic Of China-Effective Nov. 1, 2021-Digichina' (*digichina.stanford.edu*, 2021) <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> accessed 17 April 2022.

Ruth Gavison, "Privacy and the Limits of Law" (1980) 89 The Yale Law Journal 421

Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 195-197

Sangchul Park and others, "Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies" (2020) 323 JAMA 21-24

Selina Cheng, 'Hong Kong Moves To Ease Fears As Industry Group Says Facebook, Google, Twitter May Pull Out Of City Over New Privacy Law - Hong Kong Free Press HKFP' (*hongkongfp.com*, 2021) <https://hongkongfp.com/2021/07/06/hong-kong-moves-to-ease-fears-as-facebook-google-twitter-threaten-to-pull-out-of-city-over-new-privacy-law/> accessed 13 April 2022.

Sinta Dewi, 'Model Regulation for Data Privacy in the Application of Biometric Smart Card' (2017) 4 Brawijaya Law Journal

Sinta Rosadi, 'Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia' (2018) 5 Brawijaya Law Journal.

Sionaidh Douglas-Scott, "Privacy, Intimacy and Isolation. by Julie Inness" (1993) 102 Oxford University Press 655–658

Sugeng and Annisa Fitria, "Legal Protection of E-Commerce Consumers Through Privacy Data Security" (2021) Proceedings of the 1st International Conference on Law and Human Rights 2020 (ICLHR 2020) 2-4.

Terence Lee and Howard Lee, 'Tracing Surveillance And Auto-Regulation In Singapore: 'Smart' Responses To COVID-19' (2020) 177 Media International Australia.

The Government of the Hong Kong Special Administrative Region, 'Personal Data (Privacy) (Amendment) Bill 2021' (Constitutional and Mainland Affairs Bureau 2021).

Vili Lehdonvirta, 'European Union Data Protection Directive: Adequacy Of Data Protection In Singapore' (2004) Singapore Journal of Legal Studies.

World Shipping Council, 'Top 50 Ports' (*www.worldshipping.org*, 2019) <https://www.worldshipping.org/top-50-ports> accessed 18 April 2022.

Yang Feng, "The future of China's personal data protection law: challenges and prospects" (2019) 27 Asia Pacific Law Review 70.

Younsik Kim, "Uncertain future of privacy protection under the Korean public health emergency preparedness governance amid the COVID-19 pandemic" (2022) 8 Cogent Social Sciences 10-11.